БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

ФИО преподавателя: Селин А.А., канд. техн. наук

По своей природе большие базы данных никогда не будут свободны от злоупотреблений в результате нарушений безопасности. Если большая система предназначена для облегчения доступа, она становится небезопасной; если она сделана непроницаемой, то ее становится невозможно использовать.

Росс Андерсон («Правило Андерсона»)

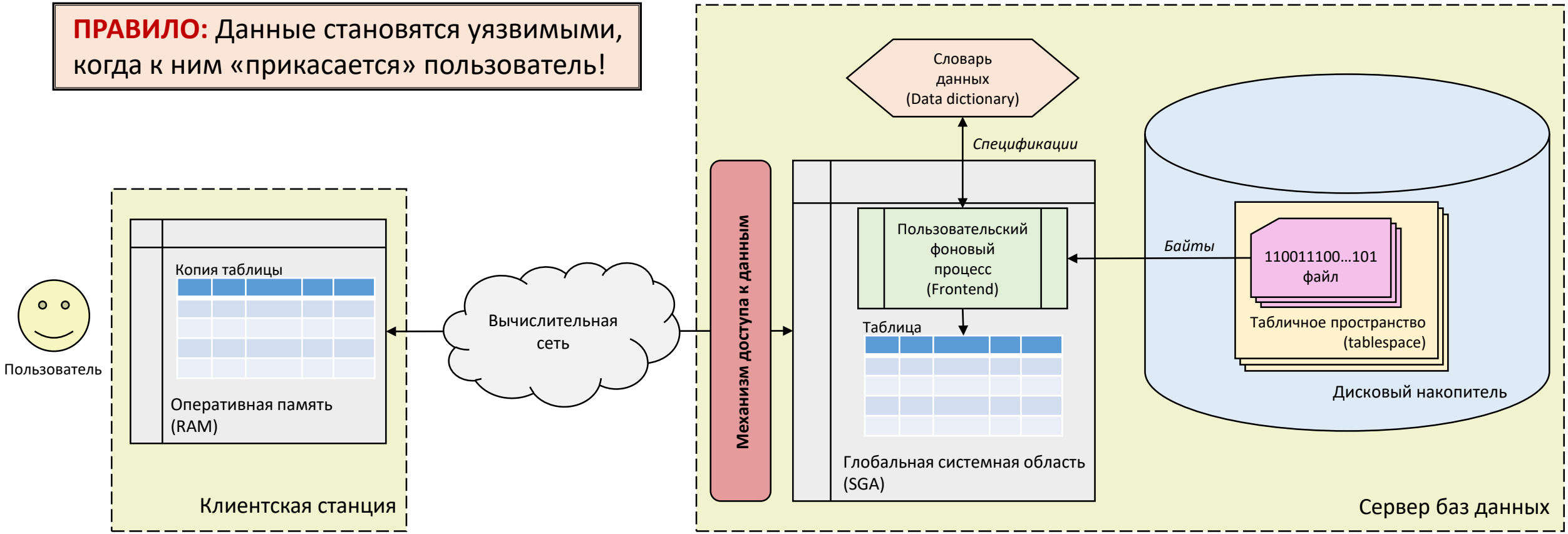
ОРГАНИЗАЦИЯ МАНДАТНОЙ ЗАЩИТЫ В СИСТЕМАХ БАЗ ДАННЫХ

Учебные вопросы:

1. Структуры хранения данных и методы доступа к ним
2. Принципы атрибутивной защиты данных
3. Аутентификация пользователя

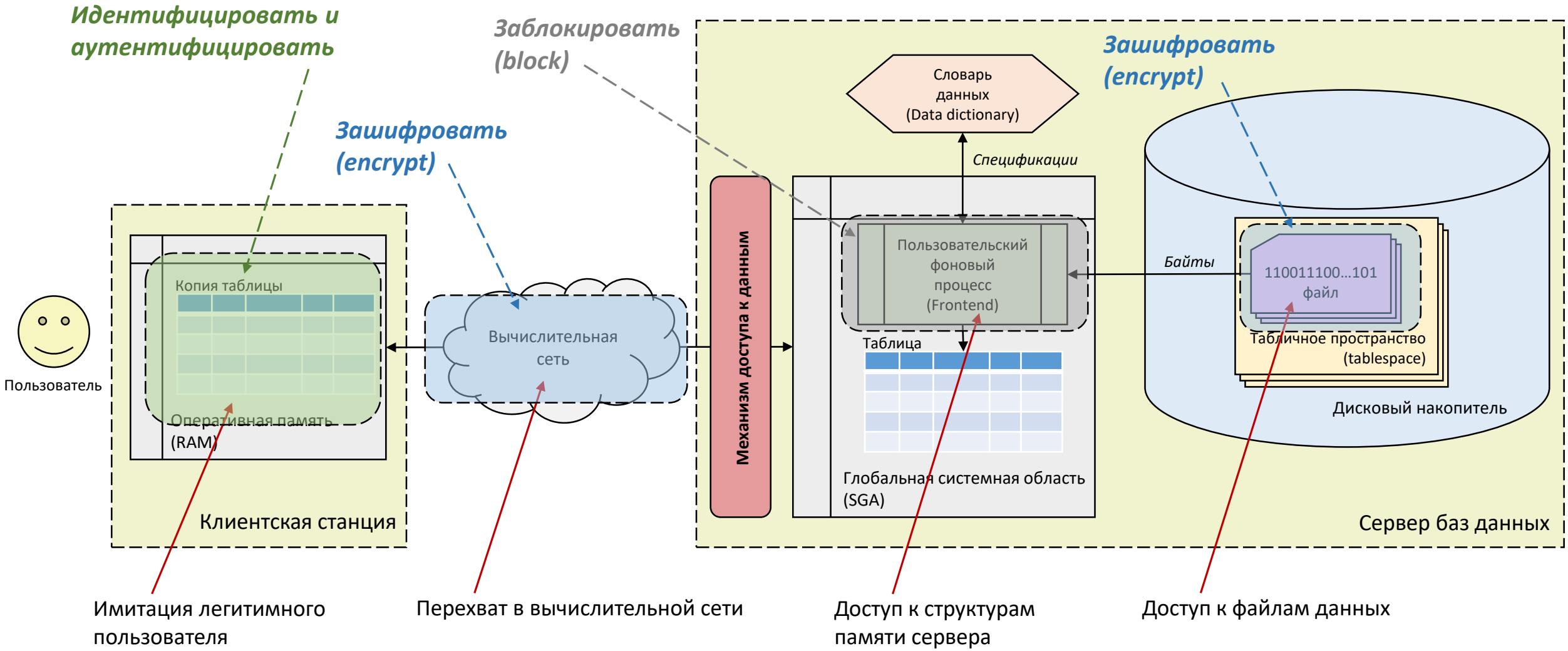
СТРУКТУРЫ ХРАНЕНИЯ ДАННЫХ И МЕТОДЫ ДОСТУПА К НИМ

ПРАВИЛО: Данные становятся уязвимыми, когда к ним «прикасается» пользователь!



Безопасный доступ к данным – подключение клиентской станции к каналу передачи копий запрошенных сегментов базы данных и посылки в систему управления базами данных текстовых команд на манипулирование хранящимися данными на встроенном языке базы данных (например, SQL).

СТРУКТУРЫ ХРАНЕНИЯ ДАННЫХ И МЕТОДЫ ДОСТУПА К НИМ

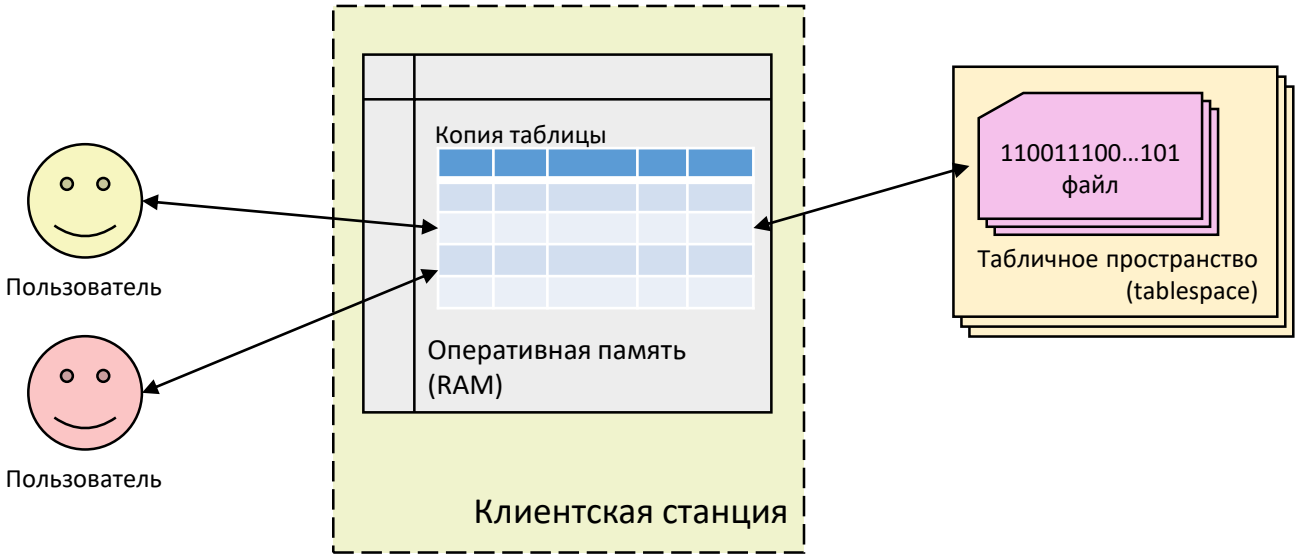


СТРУКТУРЫ ХРАНЕНИЯ ДАННЫХ И МЕТОДЫ ДОСТУПА К НИМ

Методы доступа к данным в БД:

1. **Дискреционные** (англ. *discretionary access control*, ***DAC***) — управление доступом субъектов (пользователей или прикладных процессов) к объектам (фрагментам данных, файлам, сегментам БД) на основе списков управления доступом или матрицы доступа (матрицы безопасности). *Каждому пользователю (прикладному процессу) предписывается право доступа к каждому фрагменту данных, если право не предоставлено, то его запросы к данному фрагменту данных игнорируются.*
2. **Мандатные** (англ. *mandatory access control, **MAC***) — разграничение доступа субъектов к объектам, основанное на назначении степени конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такой степени конфиденциальности. *Каждому пользователю (прикладному процессу) назначается привилегия доступа (или ограничение на доступ) к каждой степени конфиденциальности, если субъект обращается к данным со степенью конфиденциальности, к которой он не допущен, то его запросы отклоняются.*
3. **Ролевые** (англ. *role based access control, **RBAC***) — развитие методов дискреционного доступа, при этом привилегии субъектов системы на объекты группируются с учётом специфики их применения, образуя роли. *Все пользователи (прикладные процессы) объединяются в группы с одинаковым уровнем благонадежности и наследуют привилегии доступа к данным, назначенные для их уровня благонадежности.*
4. **Атрибутивные** (англ. *attribute-based access control, **ABAC***) — метод доступа к объектам, основанный на наборе правил для атрибутов объектов или субъектов, возможных операций с ними и окружения, соответствующего запросу. *Каждому уровню благонадежности пользователей (прикладных процессов) назначается совокупность привилегий и условий, при которых они реализуются, относительно каждой степени конфиденциальности данных, что позволяет учитывать условия обращения к данным, как дополнительный фактор в принятии решения о доступе.*

ПРИНЦИПЫ АТРИБУТИВНОЙ ЗАЩИТЫ ДАННЫХ



Пользователь = легитимный пользователь, прикладная программа, злоумышленник, ошибочно легитимный пользователь,..

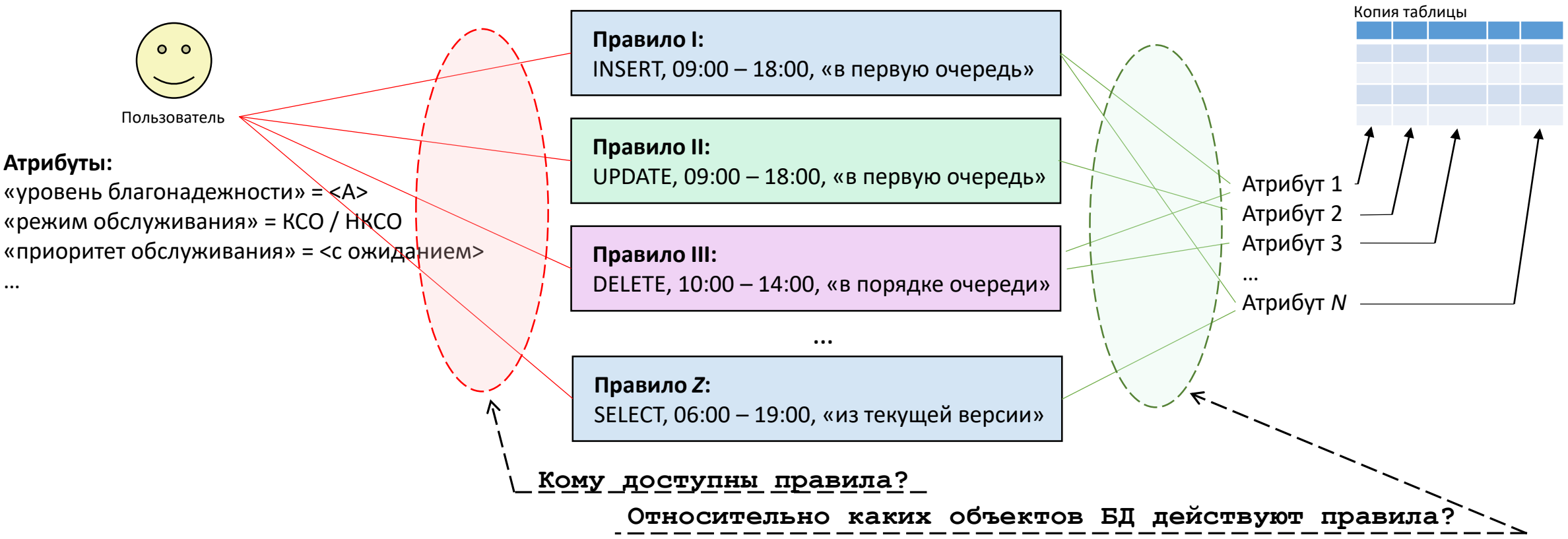
Пользователь наделяется полномочиями по «прикосновению» к **данным**

Принципы наделения пользователей полномочиями:

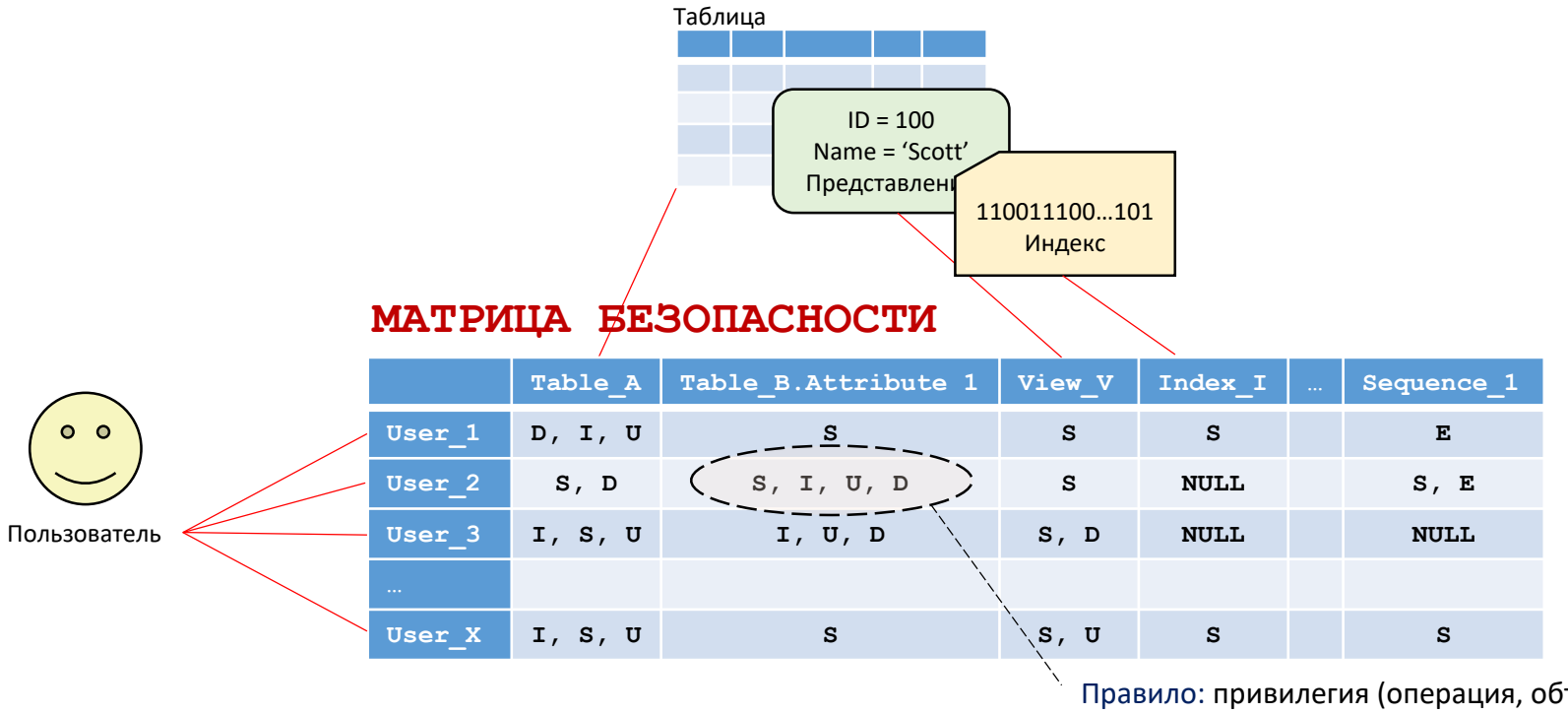
ПРИНЦИП НАИМЕНЬШЕЙ ПРИВИЛЕГИИ И РАЗДЕЛЕНИЯ ОБЯЗАННОСТЕЙ – данные должны быть тщательно распределены между исполнителями как по содержанию атрибутов, так и по набору средств их обработки (INSERT, UPDATE, DELETE, SELECT и другие возможные), особенно это касается совместно используемых данных.

ПРИНЦИП ПРЕДОСТАВЛЕНИЯ НАИМЕНЬШЕГО КОЛИЧЕСТВА ПРИВИЛЕГИЙ – каждому субъекту обработки данных должны выдаваться минимально необходимые права по обработке каждой порции данных, в идеале на каждую ячейку, на практике не каждый объект базы данных (таблицу, представление, индекс, последовательность, хранимую процедуру, функцию, триггер и т.п.).

ПРИНЦИПЫ АТРИБУТИВНОЙ ЗАЩИТЫ ДАННЫХ



ПРИНЦИПЫ АТРИБУТИВНОЙ ЗАЩИТЫ ДАННЫХ



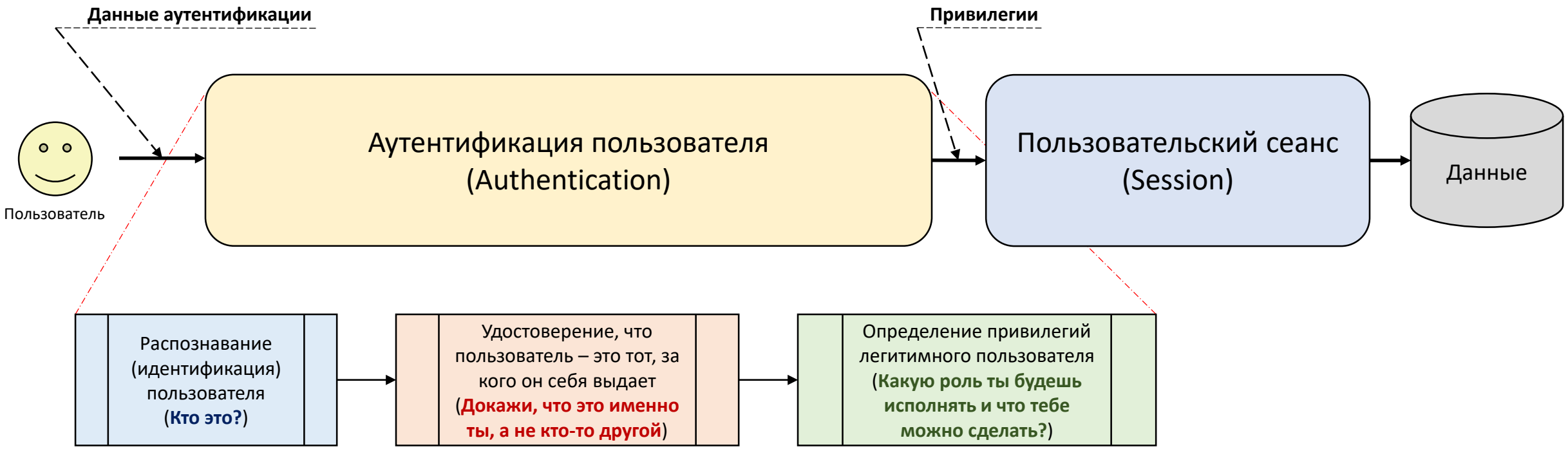
	Table_A	Table_B.Attribute 1	View_V	Index_I	…	Sequence_1
User_1	D, I, U	S	S	S		E
User_2	S, D	S, I, U, D	S	NULL		S, E
User_3	I, S, U	I, U, D	S, D	NULL		NULL
…						
User_X	I, S, U	S	S, U	S		S

Правило атрибутивной защиты данных:
Каждому субъекту обработки данных (пользователю/прикладному процессу) для каждого минимально возможного (атомарного, неделимого) объекта БД (таблицы, колонки, представления, индекса, курсора, функции, последовательности, сегмента отката, табличного пространства, сессии, …) назначается отдельная привилегия для отдельного вида операции обработки (S – выборка, U – модификация, I – вставка, D – удаление, A – преобразование структуры объекта БД, …).

```
CREATE USER [| ROLE] <Имя_учетной_записи> IDENTIFIED BY <Пароль> [<Опции>];
GRANT <Список_привилегий> TO <Имя_учетной_записи> [<Опции>];
REVOKE <Список_привилегий> FROM <Имя_учетной_записи> [<Опции>];
GRANT <Список_привилегий> ON <Имя_объекта_БД> TO <Имя_учетной_записи> [<Опции>];
```

«Чужой» объект (объект не своей схемы)

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ



ГОСТ Р ИСО/МЭК 9594-8-98 «Основы аутентификации»: формат данных аутентификации, хранимых справочником;
способ получения из справочника данных аутентификации;
способы формирования и размещения в справочнике данных аутентификации;
способы использования данных аутентификации прикладными программами;
обеспечение услуг защиты данных с помощью аутентификации.

FIPS 113 “Computer Data Authentication”: алгоритм аутентификации по данным аутентификации (Data Authentication Algorithm – DAA);
способ контроля целостности информации на основе данных аутентификации.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ

Фактор аутентификации – устойчивое свойство или характеристика субъекта доступа с оригинальными значениями набора данных аутентификации.

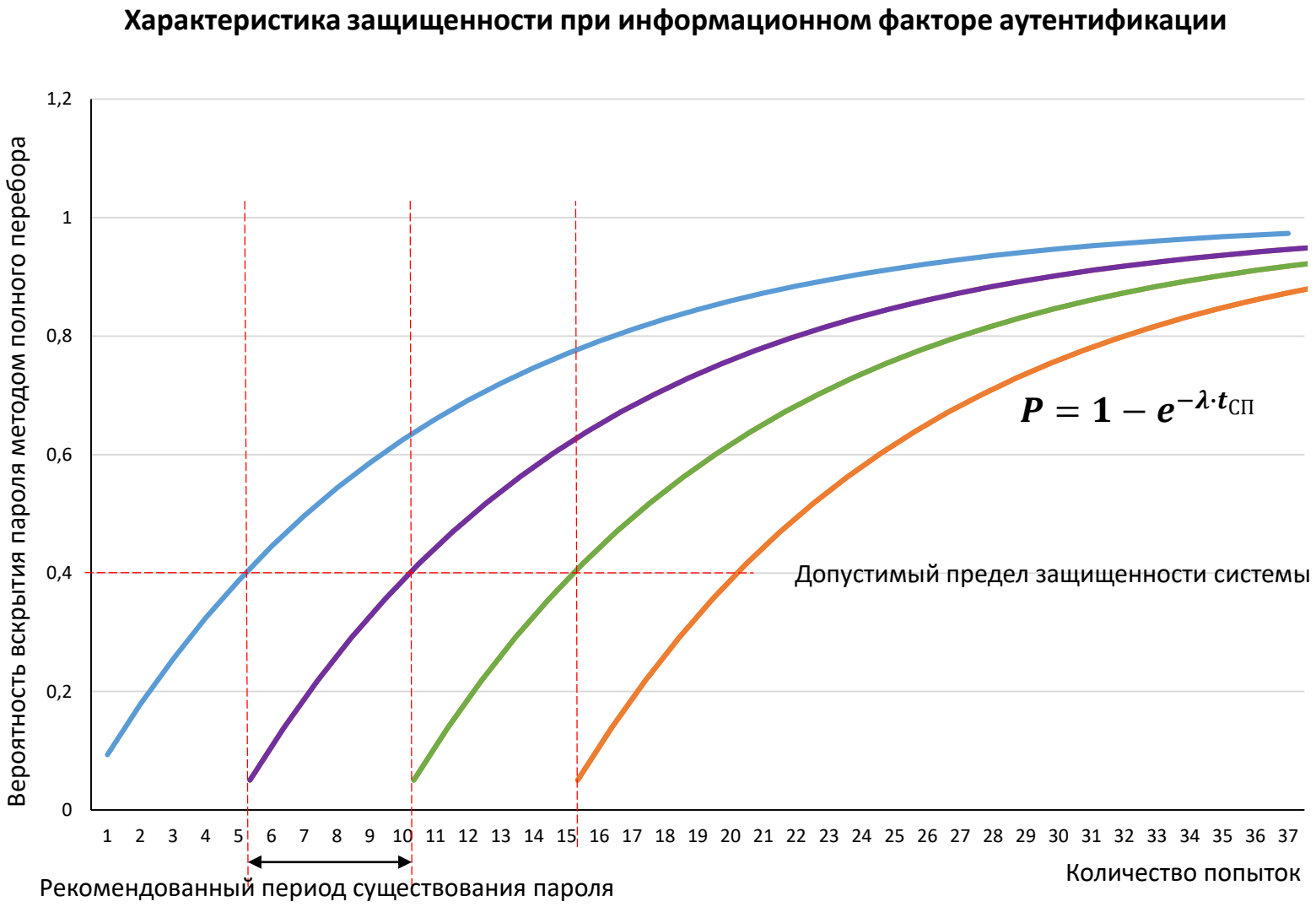
Род фактора аутентификации:

1. Информационный – нечто, что известно только субъекту доступа (пароль, PIN-код, секретное слово, тайное число, аутентификационная строка,…).
2. Физический – нечто, чем обладает субъект доступа (ключ, личная печать, файл с оригинальным набором данных на физическом носителе,…).
3. Биометрический – неотъемлемая часть субъекта доступа с оригинальным набором свойств (отпечаток пальца, радужная оболочка глаза,…).

Способы повышения защищенности базы данных на основе применения факторов аутентификации:

1. Применение средств шифрования информационного фактора (шифрование, хеширование паролей).
2. Ограничение периода действия многоразового пароля.
3. Расширение алфавита многоразового пароля.
4. Ограничение числа последовательных неудачных попыток аутентификации.
5. Использование одноразовых паролей.
6. Применение несимметричных парольных систем (электронная цифровая подпись, с публичным ключом шифрования).
7. Использование камуфляжа для средств физического управления доступом (маскировка токенов, имитация ключей, интеграция токенов в мультифункциональные устройства и тому подобное).
8. Маскировка и/или шифрование файла данных аутентификации.
9. Многофакторная аутентификация (последовательное использование разнородных факторов в разных сочетаниях).

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ



Сложность пароля (энтропия комбинации):

$$H = \log_2 N^L = L \cdot \frac{\ln N}{\ln 2} = 1.44 \cdot L \cdot \ln N$$

L – длина пароля

N – алфавит пароля (количество возможных символов)

Национальный институт стандартов и технологий (США) – NIST для оценки энтропии пароля, созданного человеком и не включающего символы из неанглийских алфавитов, предлагает использовать следующее правило:

$$H = H_1 + H_2 + \cdots + H_m \text{ , где}$$

$$H_1 = 4,\ H_2 \dots H_8 = 2,\ H_9 \dots H_{20} = 1.5,\ H_{21} \dots H_m = 1$$

Российские исследования для оценки защищенности паролем для случая, когда подбор ведется методом тотального перебора, рекомендуют исследовать величину интенсивности попыток взлома – $\boldsymbol{\lambda}$, как обратное значение возможного числа итераций алгоритма перебора.

$$\lambda = \frac{1}{N^L}$$

В этом случае при заданной защищенности (допустимой вероятности вскрытия) при известных объеме алфавита и длине пароля легко вычислить допустимый период до его смены.

Литература:

1. **Смирнов, С. Н.** Безопасность систем баз данных [Текст]: учеб. пособие для вузов по специальностям в области информационной безопасности. – М.: Гелиос АРВ , 2007. – 350 с.

2. **Федин, Ф. О.** Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — М.: РТУ МИРЭА, 2020. — Электрон. опт. диск (ISO)

3. **Терьо, М.** Oracle. Руководство по безопасности [Текст] / М. Терьо, А. Ньюмен; Пер. с англ.. — М.: Лори, 2004. — 560 с.: ил.

4. **Советов, Б. Я.** Базы данных: теория и практика : Учебник для вузов / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — М.: Высш. шк., 2005. — 464 с.: ил.

5. **Саймон, А.** Безопасность баз данных. // СУБД № 1, 1997 г. – с. 78 – 95.

6. **Кузнецов, С. Д.** Основы баз данных: курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. ин-форм. технологий / С. Д. Кузнецов. – Москва: Интернет-ун-т ин-форм. технологий, 2005. – 488 с.

7. **Смирнов, С. Н., Задворьев, И. С.** Работаем с ORACLE.: Учебное пособие/2-е изд., испр. и доп. – М: Гелиос АРВ, 2002 г. – 496 с.

8. **Кульба, В.В.** и др. Теоретические основы проектирования оптимальных структур распределенных баз данных. – М: СИНТЕГ, 1999 г. – 660 с.

9. Материалы сервера ORACLE/RE. www.oracle.ru/press/magazine/main.html

10. Материалы информационного ресурса WIKIPEDIA. https://ru.wikipedia.org/wiki/Разграничение_доступа_на_основе_атрибутов; https://ru.wikipedia.org/wiki/Аутентификация; https://ru.wikipedia.org/wiki/Многофакторная_аутентификация; https://ru.wikipedia.org/wiki/Сложность_пароля.